ARP 스푸핑을 이용한 인터넷 차단기 설계 및 구현

김수희*, 정인환
한성대학교 컴퓨터공학과
{climax79*, ihjung}@hansung.ac.kr

Design and Implementation of Internet Stopper using ARP Spoofing

Soo-Hee Kim*, In-Hwan Jung
Dept. of Computer System Engineering. Hansung University

요 약

ARP 스푸핑(spoofing) 란 ARP reply message를 동일 서브넷 상의 호스트들에게 보내어 관리자 컴퓨터가 라우터로 믿게 하는 것을 말한다. 스푸핑에 의해 패킷들이 관리자로 보내지는 상황에서 관리자가 그 패킷들을 본래 라우터로 전달하지 않고 폐기한다면 서브넷 상의 호스트들은 인터넷을 사용할 수 없는 상황이 된다. 본 논문에서는 이러한 방법을 이용하여 인터넷 차단기를 구현하였다. 구현된 인터넷 차단기는 대학교 실습실과 같은 공공의 네트워크 환경에서 필요에 의해 인터넷을 잠시 중단시킬 필요가 있는 경우 간단하게 인터넷 사용을 차단할 수 있다.

1. 서론

대학교 실습실과 같은 공공의 네트워크 환경에서 필요에 의해 잠시 인터넷을 중단시킬 필요가 있다. 예를 들어 실습실에서 시험을 보는 경우와 부득이하게 인터넷을 차단해야 할 필요가 있을 것이다. 실습실에서 교육과 상관없는 인터넷 사용에도 인터넷을 차단시켜야 할 경우가 있다. 이 경우 직접 허브나 라우터의 전원을 차단시키거나 부분적 차단을 위해 네트워크 선을 분리시키는 물리적인 방법보다 소프트웨어적인 방법이 필요하다. 본 논문에서는 이러한 상황에 맞게 간단한 방법으로 인터넷을 차단할 수 있는 인터넷 차단 시스템을 설계하고 구현하였다. 구현된 인터넷 차단기는 ARP 스푸핑(spooping) 기법을 이용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 ARP 프로토콜과 라우팅의 원리 및 본 논문의 근간이 되는 ARP 스푸핑 기법을 설명한다. 3장에서는 인터넷 차단기의 설계 및 구현에 대하여 설명한다. 4장에서는 인터넷 차단이 실험 결과를 설명한다. 마지막으로 5장에서는 결론과 향후 연구에 대하여 설명한다.

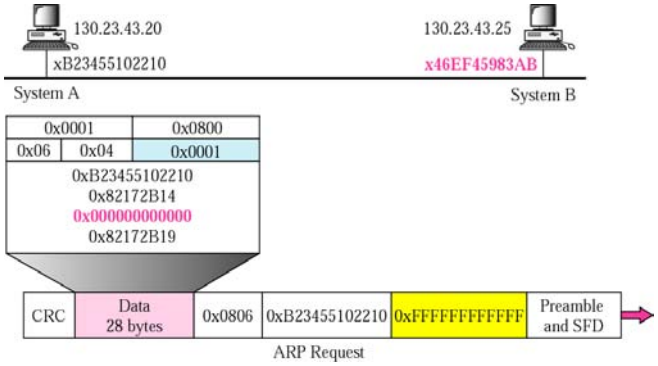
2. 관련연구

2.1 ARP 프로토콜과 라우팅의 원리

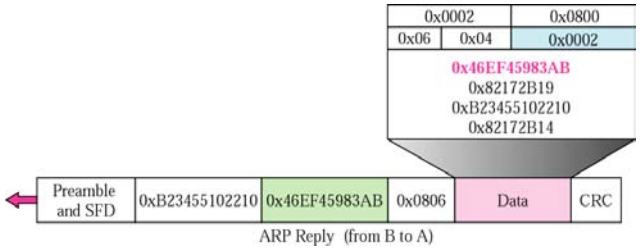
이더넷(Ethernet)[1] 환경에서 어떤 컴퓨터가 다른 호스트로 ftp나 telnet 등과 같은 네트워크 연결을 하기 위해서는 상대방 호스트의 이더넷 주소를 알아야 한다. 즉, 사용자는 IP 주소를 기반으로 연결을 하지만 이더넷 상에서는 이더넷 주소를 이용하게 된다. 이때 사용하는 프로토콜이 ARP(주소 Resolution Protocol)[2]라 한다.

네트워크상에 모든 호스트에 ARP request라고 불리는 이더넷 프레임을 보낸다. 연결하고자 하는 호스트의 IP 주소를 포함한 ARP request는 이더넷 상의 모든 호스트들에게 전송한다. ARP request를 받은 각 호스트는 자신의 IP 주소와 비교하여 해당

IP 주소를 사용하는 호스트는 자신의 하드웨어 주소(이더넷 주소)를 ARP Sender에게 보내주게 되는데 이를 ARP reply라고 한다. 이렇게 얻어진 상대방의 MAC 주소를 사용하여 인터넷이 가능하게 된다. [그림 1], [그림 2]는 ARP Request와 ARP Reply의 과정을 보여주고 있다.



[그림 1] ARP request message



[그림 2] ARP reply message

어떤 IP 서브넷에 속한 컴퓨터는 다른 서브넷과의 통신을 위해서는 라우터와 통신을 하여야 한다. 이때 그 컴퓨터는 IP 패킷에 이더넷 헤더를 붙이면서 목적지 이더넷 주소를 라우터의 MAC 주로로 채우게 된다. 그렇게 되면 그 패킷은 라우터가 읽어가게 되어 결국 라우팅에 의한 최종 목적지까지 전달이 이루어지는 것이다. 이것이 IP 라우팅의 원리이다. 본 논문에서는 PC 들이 가지고 있는 라우터의 MAC 주소를 인터넷 차단기의 MAC 주로로 대치하도록 하여 해당 PC들이 패킷을 라우터에게 전달하지 못하도록 하는 ARP 스푸핑을 사용하였다.

2.1 ARP Spoofing

위조된 ARP reply message를 Broadcast로 네트워크에 주기적으로 보내어 네트워크상의 다른 모든 호스트들이 차단기가 설치된 호스트를 라우터로 믿게 하는 것을 ARP Spoofing[3]이라 한다.

라우터의 MAC 주소는 동일 서브넷 상의 호스트가 인터넷을 사용하기 위해서 필요한 주소이다. 라우터가 호스트의 MAC 주소를 알지 못하기 때문에 Broadcasting 패킷(ARP request)을 보내게 된다. 이 패킷은 라우터 하단의 모든 호스트들이 받게 되며 이 패킷의 목적지 IP 주소에 해당하는 호스트는 자신의 MAC 주소를 기록하여 (ARP reply) 라우터에게 Unicast로 응답하게 된다.

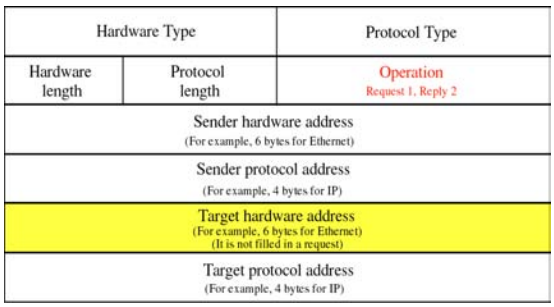
위와 같은 원리를 이용하여 차단기가 설치된 호스트는 주기적으로 ARP reply를 하단의 모든 호스트들에 보내어 라우터로 믿게 되는 것이다.

3. 설계 및 구현

본 프로그램에서 구현된 인터넷 차단기는 ARP reply message를 라우터의 MAC 주소가 아닌 차단기가 설치된 서버컴퓨터의 MAC 주소로 변환시킴으로써 인터넷 차단을 한다.

3.1 ARP reply message 설계

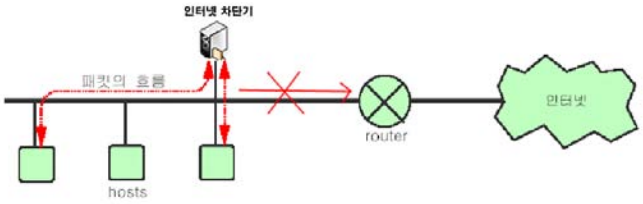
[그림 3]은 ARP Format을 보여준다. 인터넷 차단기가 설치된 호스트는 ARP request message를 보낸 호스트에게 주기적으로 ARP reply message 보내게 된다. 이때 패킷 포맷은 Operation field 02(ARP request state code)로, Target Hardware 주소 field는 인터넷 차단기가 설치된 호스트의 MAC 주소로 변환시킨다. 호스트는 라우터의 MAC 주소를 인터넷 차단기가 설치된 호스트로 인식, 모든 패킷을 그곳으로 보내게 된다.



[그림 3] ARP Format

[그림 4]와 같이 ARP 패킷을 받은 호스트들은 자신의 ARP cache를 업데이트하게 되고, 호스트 간에 연결이 일어날 때 차단기 설치 호스트에 MAC 주소를 사용하게 된다. 결국 호스트들의 모든 트래픽은

차단기 설치 호스트가 위치한 세그먼트로 들어오게 된다.



[그림 4] ARP spoofing 흐름도

3.2 응용 프로그램(Application)

ARP reply message send는 Winpcap[4]을 이용한 RAW mode packet를 이용하였다.

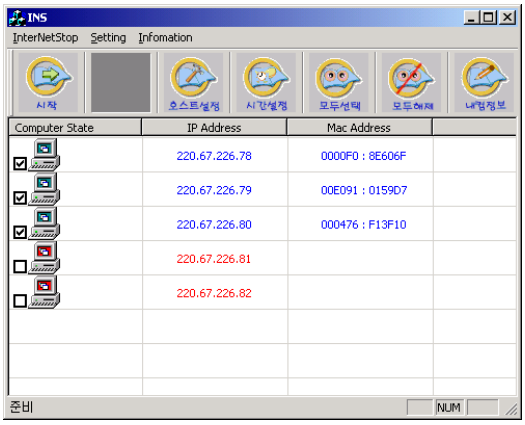
인터넷 차단기는 설치된 호스트를 기준으로 하여서 라우터 하단의 모든 호스트 ARP reply message를 보내게 된다. 본 논문에서 제안하고 구현한 내용을 기술하면 다음과 같다.

3.2.1 호스트 설정 및 라우터 정보 수집

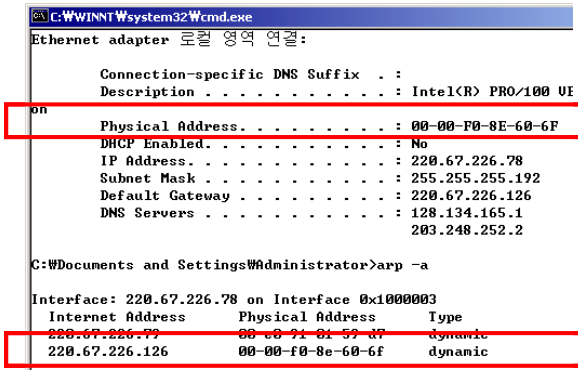
프로그램이 실행되면 우선적으로 라우터의 IP 주소와 MAC 주소를 수집하게 된다. 그 이후사용자가 인터넷을 차단하고 싶은 호스트의 범위를 설정하면 Ping Scanning 및 MAC Scanning을 통하여서 설정된 호스트의 IP 주소 및 MAC 주소, 호스트의 동작 여부를 확인하게 된다.

3.2.2 호스트 정보 표시 기능

Scanning을 마치게 되면 [그림 5]와 같이 리스트로 표시한다. 녹색은 동작중인 호스트를 의미하고, 붉은색은 중지중인 호스트를 의미한다. 만약 동작이 중지된 호스트가 다시 동작하게 되면 녹색으로 나타나게 되며 MAC 주소가 갱신된다. [그림 5]와 같이 호스트들의 IP 주소와 MAC 주소가 표시되며 체크한 호스트만이 인터넷이 차단된다. [그림 6]을 보면 차단기가 설치된 IP 주소는 220.67.226.78이며 MAC 주소는 00-00-f0-8e-60-6f 임을 알 수 있다. 라우터 Table보면 라우터의 IP 주소는 220.67.226.126이며 MAC 주소는 차단기와 동일한 MAC 주소 00-00-f0-8e-60-6f로 변경됨을 알 수 있다.



[그림 5] 프로그램 실행 화면



[그림 6] 변경된 ARP 테이블 정보

4. 실험 및 평가

4.1 실험환경

구성	사양
PC	CPU : Petium4 1.8 RAM : 256M LanCard : Intel(R) PRO/100 VE Network Connection
Network	100M Switch Hub(3Com 12port) : 4개 라우터(라우터 CISCO 2621) : 1개

네트워크에 연결된 60대의 호스트들을 대상으로 4개의 스위치 허브로 연결된 local 네트워크이다.

4.2 실험방법

네트워크로 동일한 서브넷 상의 호스트들에 대해서 IP 설정을 한 후에 ARP reply message send 방송주기 변경과 호스트 수를 변경하면서 인터넷 차단 여부를 측정하였다.

4.3 실험 결과 및 분석

대상 네트워크에 대해 평가를 측정한 결과는 아래 [표1]와 같다.

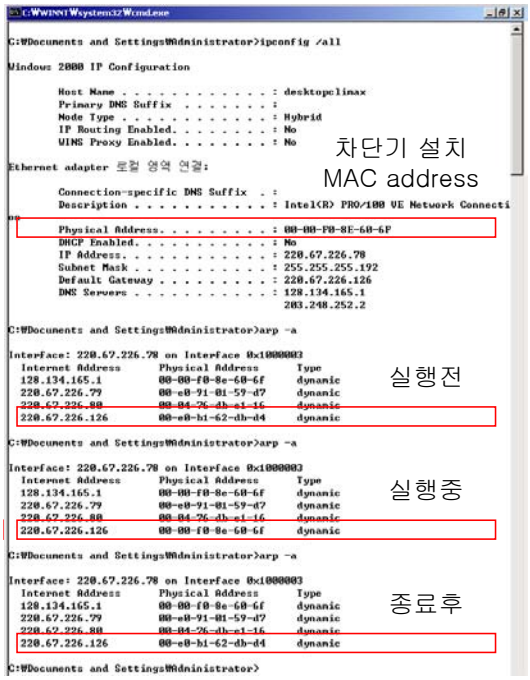
호스트수 / 방송 주기(초)	20	40	60
1	불가능	불가능	불가능
2	불가능	불가능	불가능
3	불가능	불가능	불가능
4	불가능	불가능	불가능
5	부분가능	부분가능	부분가능
6	가능	가능	가능

[표 1] 테스트 결과

ARP reply message 방송주기는 약 5초미만으로 했을 경우 인터넷이 되지 않았다. 설정시간이 약 5초가 넘어가면 차단기가 설치된 호스트보다 라우터의 ARP request에 의해서 ARP cache를 업데이트가 늦어지게 된다.

초당 보내는 패킷 데이타는 개당 60 Byte 이며 총 패킷 데이터 량은 호스트 수에 비례하였다. 하지만 패킷의 개당 용량이 얼마 되지 않으므로 인터넷 차단기가 설치된 호스트의 성능에는 지장을 주지 않는다.

ARP Spoofing이 중단되면, 계속적인 라우터의 ARP request message로 인하여 호스트의 라우터 MAC 주소가 정상적으로 복구되는 것을 확인 할 수 있었다. 전체적으로 호스트들이 인터넷이 가능하게 되는 시간은 약 5초 볼 수 있었다. 아래 [그림 6]은 차단기가 시작되어서 라우터의 맥 주소가 변경된 모습과 차단기가 해지되면서 원래의 라우터 맥 주소로 변경됨을 보여준다.



[그림 6] 실행 중 변하는 라우터의 MAC address

5. 결론 및 향후 연구

본 논문에서는 Winpcap을 이용한 RAW mode packet 전송으로 ARP Spoofing 기법이 인터넷 차단 방법으로 사용 될 수 있음을 알 수 있었다. 실험을 통하여 약 5초 미만의 주기의 ARP reply message 전송으로 완전한 인터넷 차단이 가능함을 알 수 있었다. 이 인터넷 차단기는 실습실에서 수업시간 중 학생들의 인터넷 사용을 막는 도구로 유용하게 쓰이고 있다. 향후 연구 과제는 수작업으로 IP 범위를 설정하는 대신 활동중인 PC의 MAC 주소를 자동으로 인식하는 기법을 추가하고 특정 싸이트 및 메신져를 차단하는 기능까지 추가할 예정이다. 또한 사용자 인터페이스를 보완하여 사용하기 쉽게 하는 일이다.

참고문헌

[1] Internetworking Technologies Hanadbook, EthernetTechnologies(http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc)

[2] Frederic Raynal, Eric Detoisien and Cedric Blancher, arp-sk(A swiss knife tool for ARP), April 2003

[3] Sean Whalen, An Introducation to Arp Spoofing, April 2001

[4] http://winpcap.polito.it/docs/default.htm, WinPcap Homepage

[5] Bill Woodcock, Ask Woody about Spoofing Attacks, Zocalo Engineering(http://www.netsurf.com/nsf/v01/01/local/spoof.html)

[6] CERTCC-KR, IP spoofing 공격과 대책,CERTCC-KR 기술문서(http://www.certcc.or.kr/advisory/tr/IPspoof.html)

[7] Michael Schiffman, IP-spoofing Demystified, Phrack 48-14(http://www.phrack.org/phrack/48/P48-14)